Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

Claim 1. (Currently Amended) A mobile communication terminal for providing mobile communication functions, for accessing a content server by at least one of wired and wireless communication, downloading content from the content server, and uploading the downloaded content to an external device which is not attached to the mobile communication terminal, the mobile communication terminal comprising:

a memory for storing model information and a serial number of the mobile communication terminal and the downloaded content, and also for storing an encryption key for encrypting the content downloaded from the external device;

a communication unit for providing mobile communication functions and an interface for exchanging data with the external device;

an encryption unit for encrypting the serial number and the content with the encryption key, thereby restricting use of the content to the mobile communication terminal;

a controller for uploading the encrypted content from the mobile communication terminal to the external device via the communication unit, and for transmitting a download request signal for the uploaded content to the external device in response to an input command; and

a decryption unit for decrypting, with the encryption key, the content downloaded from the external device in response to the download request signal for the uploaded content, wherein the encryption key is generated by the external device considering further time information set in the external device.

Claim 2. (Previously Presented) The mobile communication terminal of claim 1, wherein the encryption key is generated by the external device based on the model information and the serial number of the mobile terminal.

Claim 3 (Canceled)

Claim 4. (Previously Presented) A content security system comprising:

a mobile communication terminal for providing mobile communication functions, for encrypting content provided from a content server with an encryption key provided from an external device which is not attached to the mobile communication terminal, and for uploading the encrypted content from the mobile communication terminal to the external device; and

an external memory device for generating the encryption key based on model information and a serial number of the mobile terminal, and storing the encrypted content uploaded from the mobile communication terminal, thereby restricting use of the content to the mobile communication terminal, wherein the external memory device generates the encryption key considering further time information set in the external memory device.

Claim 5 (Canceled)

Claim 6. (Previously Presented) The content security system of claim 5, wherein the external memory device determines whether the time information set in the external memory device is identical to time information set in the mobile communication terminal, and generates the encryption key if the time information set in the external memory device is identical to time information set in the mobile communication terminal.

Claim 7. (Previously Presented) The content security system of claim 4, wherein the mobile communication terminal transmits a download request signal for previously uploaded content to the external memory device in response to an input command, and decrypts, with the encryption key, content downloaded from the external memory device in response to the download request signal.

Claim 8. (Currently Amended) A content protection method using a content security system having a mobile communication terminal for providing mobile communication *functions*

and downloading content from a content server and an external memory device for storing the content at a request of the mobile communication terminal, the external memory device not being attached to the mobile communication terminal, the method comprising the steps of:

transmitting a content upload request signal from the mobile communication terminal to the external memory device in response to an input command;

transmitting to the external memory device model information and a serial number of the mobile communication terminal, requested by the external memory device in response to the content upload request signal;

encrypting content to be uploaded from the mobile communication terminal with an encryption key generated by the external memory device based on the model information and the serial number, thereby restricting use of the content to the mobile communication terminal; and

transmitting the content encrypted by the encryption key from the mobile communication terminal to the external memory device, wherein the encryption key is generated by the external memory device considering further time information set in the external memory device.

Claim 9. (Previously Presented) The content protection method of claim 8, further comprising the steps of:

determining whether the encrypted content uploaded from the mobile communication terminal is identical to the content encrypted by the encryption key; and

storing the encrypted content on the external memory device if the encrypted content uploaded from the mobile communication terminal is identical to the content encrypted by the encryption key.

Claim 10. (Previously Presented) The content protection method of claim 9, further comprising the steps of:

upon receiving a download command for the previously uploaded content, transmitting a content download request signal from the mobile communication terminal to the external memory device;

if content index information for downloading is selected from content index information provided from the external memory device in response to the content download request signal, transmitting the selected content index information to the external memory device;

if encrypted content is downloaded from the external memory device according to the selected content index information, decrypting the downloaded encrypted content with the encryption key.

Claim 11 (Canceled)

Claim 12. (Previously Presented) The content protection method of claim 11, wherein the encryption key is generated when the time information set in the external memory device is identical to time information set in the mobile communication terminal.